THE HAUPTMODUL AT ELLIPTIC POINTS OF CERTAIN ARITHMETIC GROUPS

JAY JORGENSON, LEJLA SMAJLOVIĆ, AND HOLGER THEN

Abstract. Let N be a square-free integer such that the arithmetic group $\Gamma_0(N)^+$ has genus zero; there are 44 such groups. Let j_N denote the associated Hauptmodul normalized to have residue equal to one and constant term equal to zero in its q-expansion. In this article we prove that the Hauptmodul at any elliptic point of the surface associated to $\Gamma_0(N)^+$ is an algebraic integer. Moreover, for each such N and elliptic point e, we show how to explicitly evaluate $j_N(e)$ and provide the list of generating polynomials (with small coefficients) of the class fields or their subfields corresponding to the orders over the imaginary quadratic extension of rationals stemming from the elliptic points under consideration.

1. Introduction

1.1. **Some number theoretic considerations.** Let Γ be a discrete group acting on the hyperbolic upper half plane $\mathbb{H}$ such that the quotient $\Gamma\backslash\mathbb{H}$ has genus zero, and, of course, necessarily admits some cusps and elliptic points. The function field associated to $\Gamma\backslash\mathbb{H}$ has transcendence degree one and is generated over the field of constants, which for this paper are the complex numbers $\mathbb{C}$, by a single indeterminant which we denote by j_Γ. In general, one can normalize j_Γ by choosing a distinguished point P on $\Gamma\backslash\mathbb{H}$ and requiring j_Γ to have a first order pole at P with residue equal to one as well as zero constant term in its Laurent expansion about P having chosen a local coordinate at P.

In the specific case when $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$, we can take $P = i\infty$ since as a Riemann surface the quotient space $\mathrm{PSL}(2,\mathbb{Z})\backslash\mathbb{H}$ has a cusp. Let z denote the global coordinate on $\mathbb{H}$, and set $q = e^{2\pi iz}$ which is a local coordinate about $i\infty$. Then the (classical) j-invariant $j(z) = j_{\mathrm{PSL}(2,\mathbb{Z})}(z)$ admits the q-expansion on $\mathbf{P}^1$ given by

$$j(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_k q^k = \frac{1}{q} + 744 + 196884q + 21493760q^2 + O(q^3) \quad \text{as } q \to 0. \tag{1}$$

From the point of view of automorphic forms, j can be realized as a rational function of holomorphic Eisenstein series of weight four and six.

As it turns out, the function $j(z)$ satisfies many amazing properties. T. Schneider proved in [22] that if $\tau \in \mathbb{H}$ is an imaginary quadratic number then $j(\tau)$ is an algebraic integer. In addition, if τ is an algebraic number but not imaginary quadratic then $j(\tau)$ is transcendental; see also [24]. In modern language, the points $\tau \in \mathbb{H}$ which are imaginary quadratic numbers are called *complex multiplication points,* or CM points. In [25] it is shown how to compute $j(\tau)$ at any CM point, thus giving some fantastic formulae such as

$$j(i) = 1728, \quad j((1+\sqrt{-7})/2) = -3375, \quad \text{and} \quad j((1+\sqrt{-163})/2) = 640320^3.$$

The third example combines with (1) to yield the curiosity that the transcendental number $e^{\pi\sqrt{163}}$ is very close to an integer, a result which is attributed to Hermite.

More generally, the *singular moduli* of the j-invariant, which by definition are the values of the function j at imaginary quadratic arguments, play a very important role in the class field theory of imaginary quadratic fields; see [3]. Namely, let K be an imaginary quadratic field over $\mathbb{Q}$, of discriminant d_K and let $\mathcal{O}$ be a certain order in K. Then for an imaginary quadratic argument $\tau \in \mathbb{H} \cap \mathcal{O}$, the singular modulus $j(\tau)$ is an algebraic integer. Moreover, the extension $K[j(\tau)]$ is the ring class field of $\mathcal{O}$, which is the Hilbert class field if $\mathcal{O}$ is the maximal order of K, and can be realized constructively as the splitting field over $\mathbb{Q}$ of the class polynomial, by which we mean the minimal polynomial of $j(\tau)$.

The seminal work of Gross-Zagier [11] studies the factorization of the difference of two singular moduli $j(\tau_1) - j(\tau_2)$, from which we have a considerable amount of current research that reaches in various directions of algebraic and arithmetic number theory including special values of L-functions and the Birch-Swinnerton-Dyer conjecture, one of the six unsolved Millennium Prize Problems.

Thus, properties of the j-invariant for $\mathrm{PSL}(2,\mathbb{Z})$ play a role in algebraic number theory.

J. J. acknowledges grant support from NSF and PSC-CUNY grants.

1.2. **Connections to other fields.** Let f be a holomorphic function of one complex variable. The *Schwarzian derivative* $S(f)$ of f is a classically defined function given by

$$S(f)(z) = \left(\frac{f''(z)}{f'(z)}\right)' - \frac{1}{2}\left(\frac{f''(z)}{f'(z)}\right)^2,$$

where, as is the convention, the prime $'$ denotes differentiation with respect to the holomorphic parameter z. If f and g are holomorphic functions, then the Schwarzian of the composition $f \circ g$ satisfies the relation

$$S(f \circ g) = (S(f) \circ g)(g')^2 + S(g).$$

In addition, one can show that $S(g) = 0$ if and only if g is a fractional linear transformation. Therefore, if the function f is a holomorphic automorphic form with respect to some discrete group $\Gamma \subseteq \mathrm{PSL}(2,\mathbb{R})$, then the Schwarzian $S(f)$ is a meromorphic automorphic form of weight four with respect to Γ.

In [20] it is proven that the classical j-invariant for $\mathrm{PSL}(2,\mathbb{Z})$ satisfies the differential equation

$$S(j)(z) + R(j(z))(j'(z))^2 = 0, \tag{2}$$

where

$$R(y) = \frac{y^2 - 1968y + 2654208}{2y^2(y-1728)^2}.$$

Recently Freitag and Scanlon [10] used (2) to define a non-$\aleph_0$-categorical strongly minimal set with trivial forking geometry, thus answering an open problem about the existence of such sets. The authors in [10] attribute the question to Lascar, who himself credits the question to Poizat. We refer the reader to [10] for precise statements as well as numerous applications of their result.

Thus, properties of the j-invariant for $\mathrm{PSL}(2,\mathbb{Z})$ provide a means by which one can address problems in logic and differential algebraic geometry.

1.3. **Some other genus zero groups.** For any positive integer N, let

$$\Gamma_0(N)^+ = \left\{ e^{-1/2}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) : \quad ad - bc = e, \quad a,b,c,d,e \in \mathbb{Z}, \quad e \mid N,\ e \mid a,\ e \mid d,\ N \mid c \right\}$$

and let $\overline{\Gamma_0(N)^+} = \Gamma_0(N)^+/\{\pm \mathrm{Id}\}$, where Id denotes the identity matrix. It has been shown that there are 43 square-free integers $N > 1$ such that the quotient space $X_N := \overline{\Gamma_0(N)^+}\backslash\mathbb{H}$ has genus zero (see [9]); note that $\mathrm{PSL}(2,\mathbb{Z}) = \overline{\Gamma_0(1)^+}$. We will also say that $\Gamma_0(N)^+$ is a genus zero group if N corresponds to one of the 44 aforementioned numbers. For each such genus zero group, the surface X_N has one cusp which we can take to be at $i\infty$ and width one. Basic properties of $\Gamma_0(N)^+$, for square-free N are derived in [15] and references therein.

For every genus zero group $\Gamma_0(N)^+$ there exists a unique holomorphic modular form on $\mathbb{H}$ with a pole at $i\infty$ of order one such that its q-expansion is normalized so it begins with $1/q$ and the constant term is equal to zero. We denote the form by $j_{\Gamma_0(N)^+} := j_N$ and, following classical and well-accepted terminology, refer to j_N as the Hauptmodul of $\Gamma_0(N)^+$. Therefore, each Hauptmodul j_N possesses a Fourier expansion at the cusp $i\infty$ with integer coefficients $a_N(k)$, normalized so that $a_N(-1) = 1$ and $a_N(0) = 0$. In other words, the q-expansion of $j_N(z)$ is given by

$$j_N(z) = \frac{1}{q} + \sum_{k=1}^{\infty} a_N(k) q^k = \sum_{k=-1}^{\infty} a_N(k) q^k. \tag{3}$$

Since X_N has genus zero, the function field has transcendence degree one over $\mathbb{C}$ and is generated by one indeterminant meaning that every $\Gamma_0(N)^+$-invariant meromorphic function can be written as a rational function in j_N.

1.4. **The beginning of "monstrous moonshine".** Let $\mathbb{M}$ denote "the monster" group, which is the largest sporadic finite simple group. In the mid-1900's, there were two very important and independent observations; A. Ogg showed that the set of primes which appear in the factorization of the order of $\mathbb{M}$ is the same set of primes such that $\Gamma_0(p)^+$ has genus zero, and J. McKay pointed out that the linear-term coefficient in (1) is the sum of the two smallest irreducible character degrees of $\mathbb{M}$. Subsequent work by J. Thompson resulted in specific conjectures asserting all coefficients in the expansion (1) are related to the dimensions of the components of a graded module admitting action by $\mathbb{M}$. More generally, J. Conway and S. Norton established the "monstrous moonshine" conjectures in [6] which more precisely formulated relations between $\mathbb{M}$ and the j-invariants for the genus zero groups $\Gamma_0(N)^+$, culminating in the celebrated work of Borcherds in [2].

Thus, properties of the j-invariants j_N for the genus zero groups $\Gamma_0(N)^+$ appear in group theory and all the numerous fields touched by "monstrous moonshine".

1.5. **Singular moduli for $\Gamma_0(N)^+$.** For $N > 1$ such that $\Gamma_0(N)^+$ has genus zero, the singular moduli were studied by I. Chen and N. Yui [4]. Analogous to Schneider's result, the authors in [4] proved that if τ is a CM point satisfying $az^2 + bz + c = 0$ with $(a, N) = 1$ then the singular moduli $j_N(\tau)$ is an algebraic integer. Furthermore, if we put $K = \mathbb{Q}[\tau]$, $b^2 - 4ac = m^2 d_K < 0$, and let $\mathcal{O}$ denote the order in K of discriminant $m^2 d_K$, then Theorem 3.7.5.(2) from [4] states that for prime levels N, and assuming that $(a, N) = 1$, the singular moduli $j_N(\tau)$ generates over K the ring class field of an imaginary quadratic order $\mathcal{O}'$ of discriminant $(mN)^2 d_K$. The assumption requiring that $(a, N) = 1$ was crucial in the proof. If $(a, N) > 1$, then $K[j_N(\tau)]$ is a proper subfield of the ring class field of $\mathcal{O}'$.

The results from [4] were expanded upon in [8] and [5]. Let us denote by $\Gamma_0(N)^*$ the subgroup of $\mathrm{PSL}(2, \mathbb{R})$ generated by $\overline{\Gamma_0(N)} = \Gamma_0(N)/\{\pm \mathrm{Id}\}$ and the Fricke involution $\gamma_N = \begin{pmatrix} 0 & -1/\sqrt{N} \\ \sqrt{N} & 0 \end{pmatrix}$. Note that for prime levels N, one has $\Gamma_0(N)^* = \overline{\Gamma_0(N)^+}$, otherwise $\Gamma_0(N)^*$ is a proper subgroup of $\overline{\Gamma_0(N)^+}$. When N is a product of r primes, $\overline{\Gamma_0(N)}$ is a subgroup of index 2^r in $\overline{\Gamma_0(N)^+}$ (see e.g. [1], Lemma 9) while $\overline{\Gamma_0(N)}$ is a subgroup of index 2 in $\Gamma_0(N)^*$, hence $\Gamma_0(N)^*$ is a subgroup of index 2^{r-1} in $\overline{\Gamma_0(N)^+}$. In [8] it is proven that for any fixed elliptic point $\tau_\gamma \in \mathbb{H}$ with corresponding order two elliptic element $\gamma \in \Gamma_0(N)^* \setminus \overline{\Gamma_0(N)}$, the field $\mathbb{Q}[\tau_\gamma, j_N(\tau_\gamma)]$ is the ring class field of the order $\mathcal{O}_\gamma$ in K, where $\mathcal{O}_\gamma$ denotes the order in $K = \mathbb{Q}[\tau_\gamma]$ generated by the complex lattice $[1, \tau_\gamma]$. A similar statement is proven in [5], Theorem 4, with j_N replaced by an appropriately normalized Hauptmodul for the genus zero group $\Gamma_0(N)^*$.

The articles [4], [8] and [5] do not address the question whether the value of $j_N(\tau_\gamma)$ for any *elliptic fixed point* τ_γ of $\Gamma_0(N)^+$ is an algebraic integer. Partial numerical evidence supporting this question is given in [8]. If the answer to this question is affirmative, then, a natural follow-up problem would be to determine their minimal polynomials whose splitting fields over the appropriate extension of the rationals would be the ring class fields of the corresponding orders.

1.6. **Our results.** The main purpose of this paper is to answer the two questions posed above. We prove for all genus zero groups $\Gamma_0(N)^+$ and for all corresponding elliptic points e that the singular moduli $j_N(e)$ is an algebraic integer. Moreover, we obtain an exact evaluation in terms of radicals of each such singular moduli after which we compute the minimal polynomials of the corresponding ring class fields and their subfields.

Our analysis begins by studying (2) for any genus zero group $\Gamma_0(N)^+$. It is not difficult to show that for any Hauptmoduli f on any genus zero group Γ commensurable with $\mathrm{PSL}(2, \mathbb{Z})$ there exists a rational function $R_\Gamma(y)$ such that

$$S(f)(z) + R_\Gamma(f(z))(f'(z))^2 = 0;$$

see, for example, [12], Theorem 1.1. In this paper, we specialize to the genus zero "moonshine groups" $\Gamma_0(N)^+$ with square-free N. To be precise, we explicitly compute the rational function $R_N(y)$ such that

$$S(j_N)(z) + R_N(j_N(z))(j_N'(z))^2 = 0.$$

The analysis and algorithms presented in this article yield the following results.

Main Theorem *With the above notation, we write $R_N = P_N/Q_N$ for polynomials P_N and Q_N.*

(1) The polynomial P_N is a monic polynomial with $\deg(P_N) = \deg(Q_N) - 2$. Furthermore,

$$Q_N(j_N(z)) = 2 \prod_{e \in \mathcal{E}_N} (j_N(z) - j_N(e))^2$$

where $\mathcal{E}_N$ is the set of inequivalent elliptic points on $\mathbb{H}$ with respect to the action by $\Gamma_0(N)^+$.

(2) The coeffients of P_N and Q_N are integers.

(3) If we write $Q_N = 2(h_N)^2$, then h_N is a monic polynomial with integer coefficients, thus the values of $j_N(e)$ for $e \in \mathcal{E}_N$ are algebraic integers.

The factorization of polynomials $h_N(y)$ into irreducible polynomials over $\mathbb{Z}$ is given in Table 1. Using the q-expansions of j_N, which were obtained in [16], we then derived a list of approximate values of $j_N(e)$ for $e \in \mathcal{E}_N$, as well as the roots of h_N in terms of radicals; see appendices of [19], where the list of polynomials P_N and Q_N is also given. Finally, by pairing the values of the roots with the approximate values of $j_N(e)$, we obtained the minimal polynomials associated to each value of $j_N(e)$. After the above mentioned computations, we combine with results from [8] in order to explicitly construct the class fields of certain orders and their subfields. A summary of these results is stated in Corollary 7 and Table 2 and Table 3. For some class fields we get more than one

generating polynomial. For example for the class field of the order $\mathbb{Z}[\sqrt{-17}]$, we have three generating polynomials over $\mathbb{Q}[\sqrt{-17}]$:

$$h_{17,-4\cdot 17} = y^4+2y^3-39y^2-176y-212,\ h_{51,-4\cdot 17} = y^4+2y^3+3y^2-2y+1,\ \text{and}\ h_{119,-4\cdot 17} = y^4+2y^3+3y^2+6y+5.$$

The notation $h_{N,D}$ is defined in section 5. Those polynomials are all generating polynomials, with small coefficients, of the Hilbert class field over $\mathbb{Q}[\sqrt{-17}]$.

In the case when the level is 71, our computations agree with the results of [8], Section 4, since in this case we get the same generating polynomials of the Hilbert class field of $\mathbb{Q}[\sqrt{-71}]$.

1.7. **Outline of the paper.** In section 2 we cite results from the literature needed for our paper. In section 3 we study properties of the Schwarzian derivative $S(j_N)$ of j_N, ultimately proving part (1) of the Main Theorem. In section 4 we describe an algorithm by which we evaluate the coefficients of P_N and Q_N, and compute the polynomial h_N where $Q_N = 2h_N^2$. A complete list of all the polynomials h_N is given in Table 1. Finally, in section 5 we discuss the applications of our results to explicit class field theory. The result is stated in Corollary 7 to which we refer the reader for a precise statement.

1.8. **Computer assistance.** Computer algebra was used to assist our computations. Taking results from [16, 17, 18] for the Hauptmoduli, we used symbolic algebra of PARI/GP [21] to perform most of the algorithm of section 4. Since we had it readily available, we used our own C-code linked against the GMP Bignum Library [13] to solve (6a) in rational arithmetic for the polynomials P_N and Q_N. Moreover, in order to produce a part of the data in Table 2 below, related to even levels N, we used Alnuth package of GAP [14] to determine whether some irreducible factors of h_N generate the same field as factors of h_m, for some odd divisor m of N.

2. Background material

2.1. **Holomorphic modular forms.** Let Γ be a Fuchsian group of the first kind. Following [23], we define a weakly modular form f of weight $2k$ for $k \geq 1$ associated to Γ to be a function f which is meromorphic on $\mathbb{H}$ and satisfies the transformation property

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Assume that Γ has at least one class of parabolic elements. By transforming coordinates, if necessary, we may always assume that the parabolic subgroup of Γ has a fixed point at $i\infty$, with identity scaling matrix. In this situation, any weakly modular form f will satisfy the relation $f(z+1) = f(z)$, so we can write

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n \quad \text{where } q = e^{2\pi i z}.$$

If $a_n = 0$ for all $n < 0$, then f is said to be holomorphic in the cusp. A holomorphic modular form with respect to Γ is a weakly modular form which is holomorphic on $\mathbb{H}$ and in all of the cusps of Γ. A holomorphic modular form with respect to Γ is called a cusp form, if $a_n = 0$ for all $n \leq 0$.

2.2. **Modular forms on surfaces X_N.** From Proposition 7, page II-7, of [3], we immediately obtain the following Riemann-Roch type formula which relates the number of zeros of a modular form, counted with multiplicity, with its weight and volume of X_N.

Proposition 1. *Let f be a modular form on X_N of weight $2k$, not identically zero. Let $\mathcal{F}_N$ denote the fundamental domain of X_N and let $v_z(f)$ denote the order of zero z of f, or minus the order of pole of f. Then,*

$$k\frac{\mathrm{Vol}(X_N)}{2\pi} = v_{i\infty}(f) + \sum_{e\in\mathcal{E}_N} \frac{1}{\mathrm{ord}(e)} v_e(f) + \sum_{z\in\mathcal{F}_N\setminus\mathcal{E}_N} v_z(f),$$

where $\mathcal{E}_N$ denotes the set of elliptic points in $\mathcal{F}_N$ and $\mathrm{ord}(e)$ is the order of the elliptic point $e \in \mathcal{E}_N$.

3. Determining the polar structure of $S(j_N)/(j_N')^2$

We begin with the following elementary proposition.

Proposition 2. *For any square-free N such that the group $\Gamma_0(N)^+$ has genus zero, the function $S(j_N)(z)(j_N'(z))^2$ on $\mathbb{H}$ is a weight eight modular form with respect to $\Gamma_0(N)^+$ and is holomorphic function on $\mathbb{H}$ whose only pole is at $i\infty$ with order two. Furthermore, the q-expansion of $S(j_N)(z)(j_N'(z))^2$ is given by*

$$S(j_N)(z)(j_N'(z))^2 = (2\pi)^4\left(-\frac{1}{2q^2}+\sum_{k=0}^{\infty} b_N(k)q^k\right), \tag{4}$$

where, in the notation of (3),

$$b_N(k) = -(k+1)[(k+1)^2+3(k+1)+1]a_N(k+1)+\frac{1}{2}\sum_{l=1}^{k-1} l^2(k-l)(5l-3k)a_N(l)a_N(k-l).$$

Proof. Since

$$S(j_N)(z)(j_N'(z))^2 = j_N'''(z)j_N'(z)-\frac{3}{2}(j_N''(z))^2,$$

it is immediate that the function $S(j_N)(z)(j_N'(z))^2$ is holomorphic on $\mathbb{H}$ with the only pole at $i\infty$ of order two. From the discussion in section 1.2, we conclude that the Schwarzian $S(j_N)$ is a meromorphic modular form of weight four associated to $\Gamma_0(N)^+$. Since $j_N'(z)$ is a meromorphic weight two form, we conclude that $S(j_N)(z)(j_N'(z))^2$ has weight eight.

Beginning with the q-expansion (3) we derive the q-expansion of the lth derivative $j_N^{(l)}(z)$ for $l \geq 1$, namely the expansion

$$j_N^{(l)}(z) = (2\pi i)^l\left(\frac{(-1)^l}{q}+\sum_{k=1}^{\infty} k^l a_N(k)q^k\right),$$

hence

$$S(j_N)(z)(j_N'(z))^2 = (2\pi)^4\left(-\frac{1}{q}+\sum_{k=1}^{\infty} k^3a_N(k)q^k\right)\left(-\frac{1}{q}+\sum_{k=1}^{\infty} ka_N(k)q^k\right)-\frac{3}{2}(2\pi)^4\left(\frac{1}{q}+\sum_{k=1}^{\infty} k^2a_N(k)q^k\right)^2.$$

A straightforward computation yields (4). □

Corollary 3. *For any square-free N such that the group $\Gamma_0(N)^+$ has genus zero, the function $S(j_N)(z)/(j_N'(z))^2$ is a weight zero modular form on X_N whose zero at $i\infty$ has order two.*

We now use Proposition 1 in order to determine the set of zeros of the weight two form $j_N'(z)$ and corresponding multiplicities. From an inspection of tables given in [9], we conclude that for all square-free N such that the surface X_N has genus zero, the set $\mathcal{E}_N$ of elliptic points of X_N consists of a certain number of order two elliptic points and possibly one point of order three, four or six. For $n \in \{3,4,6\}$, we define the symbol $\delta_{n,N}$ to be equal to one if there exists an elliptic point on X_N of order n and set $\delta_{n,N}=0$ otherwise.

Proposition 4. *Let N be a square-free number such that the surface X_N has genus zero. Then the set of zeros of j_N' is equal to the set $\mathcal{E}_N$ of elliptic points of X_N. In the case when X_N has no order four or six elliptic points, the order $m_N(e)$ of every zero $e \in \mathcal{E}_N$ of j_N' is $\mathrm{ord}(e)-1$. In the case when X_N has one order four or six elliptic point, then either the order of all zeros $e \in \mathcal{E}_N$ is $\mathrm{ord}(e)-1$, or the order of all but one zero at order two elliptic points is one, there is an order two zero of j_N' at some order two elliptic point and the order of zero at order four or six elliptic point is one or two respectively.*

Proof. Let $\mathcal{E}_{2,N}$ denote the set of elliptic points of X_N of order two. If we insert $k=1$ into Proposition 1 and combine it with the Gauss-Bonet formula for the volume of X_N we arrive at the equation

$$-1+\sum_{e\in\mathcal{E}_{2,N}}\frac{1}{2}+\delta_{n,N}\frac{n-1}{n} = -1+\sum_{e\in\mathcal{E}_{2,N}}\frac{v_e(j_N')}{2}+\delta_{n,N}\frac{v_{e_{n,N}}(j_N')}{n}+\sum_{z\in\mathcal{F}_N\setminus\mathcal{E}_N} v_z(j_N'), \tag{5}$$

for $n \in \{3,4,6\}$, where we denoted by $e_{n,N}$ the order n elliptic point of X_N, if it exists.

The form j_N' vanishes at all $e \in \mathcal{E}_{2,N}$, since the transformation rule for j_N' and arbitrary order two elliptic element $\eta \in \Gamma_0(N)^+$ with fixed point e reduces to

$$j_N'(\eta(e)) = j_N'(e) = (i)^2 j_N'(e)$$

which implies that $j'_N(e) = 0$. In other words, $v_e(j'_N) \geq 1$ for all $e \in \mathcal{E}_{2,N}$. From (5), we have that $v_z(j'_N) = 0$ for all $z \in \mathcal{F}_N \setminus \mathcal{E}_N$. In the case when N is such that the surface X_N possesses no order four or six elliptic points, we immediately deduce that the order of zero $e \in \mathcal{E}_N$ is $\mathrm{ord}(e) - 1$. In the case when $\delta_{4,N} = 1$, either order of all zeros $e \in \mathcal{E}_N$ of j'_N is $\mathrm{ord}(e) - 1$, or, writing $3/4$ as $1/2 + 1/4$ we deduce that there is an order two elliptic point $e' \in \mathcal{E}_N$ which is the order two zero of j'_N and the order of zero at the order four elliptic point $e_{4,N}$ of X_N is one. A similar argument proves the statement in the case when X_N has one order six elliptic point. □

We can now determine the number and location of poles of the meromorphic modular form $S(j_N)(z)/(j'_N(z))^2$.

Proposition 5. *Let N be a square-free number such that the group $\Gamma_0(N)^+$ has genus zero. Then, the set of poles of the meromorphic modular form $S(j_N)(z)/(j'_N(z))^2$ is exactly the set $\mathcal{E}_N$ of elliptic points of X_N. Moreover, each pole has the order equal to $2(m_N(e) + 1)$, where $m_N(e)$ denotes the order of the elliptic point e as a zero of j'_N.*

Proof. We write

$$\frac{S(j_N)(z)}{(j'_N(z))^2} = \frac{j'''_N(z)j'_N(z) - \frac{3}{2}(j''_N(z))^2}{(j'_N(z))^4}.$$

Obviously, $S(j_N(z))$ is holomorphic everywhere, except eventually at zeros of $j'_N(z)$. Therefore, by Proposition 4, the set of poles of $S(j_N)(z)/(j'_N(z))^2$ is exactly $\mathcal{E}_N$.

If $e \in \mathcal{E}_N$ is a zero of j'_N of order $m_N(e)$, then by studying the power series expansion about e we see that $j'''_N(z)j'_N(z) - \frac{3}{2}(j''_N(z))^2$ is a weight eight meromorphic form with zero at e of order $2(m_N(e) - 1)$. In particular, if $m_N(e) = 1$ then the form is non-vanishing at e. Therefore, the order of the pole of $S(j_N)(z)/(j'_N(z))^2$ at $e \in \mathcal{E}_N$ is

$$4m_N(e) - 2(m_N(e) - 1) = 2(m_N(e) + 1),$$

as claimed. □

Theorem 6. *For any square-free N such that the group $\Gamma_0(N)^+$ has genus zero, there exists an integer $n_N \geq 1$ and polynomials P_N and Q_N of degrees n_N and $n_N + 2$ respectively such that*

$$\frac{S(j_N)(z)}{(j'_N(z))^2} = -\frac{P_N(j_N(z))}{Q_N(j_N(z))} = -R_N(j_N(z)). \tag{6}$$

Moreover, we may take

$$Q_N(y) = 2 \prod_{e \in \mathcal{E}_N} (y - j_N(e))^2. \tag{7}$$

which implies that the lead coefficient of P_N is equal to one and

$$n_N \leq 2 \left(\sum_{e \in \mathcal{E}_N} 1 - 1 \right). \tag{8}$$

Proof. Since j_N is the Hauptmodul, Corollary 3 implies that

$$\frac{S(j_N)(z)}{(j'_N(z))^2} = \frac{S(j_N)(z)(j'_N(z))^2}{(j'_N(z))^4} = -\frac{P_m(j_N)}{Q_r(j_N)},$$

for some polynomials P_m and Q_r of degrees m and r. The fact that $S(j_N)(z)/(j'_N(z))^2$ possesses a zero at $i\infty$ of order two, together with the expansion (3) yields that $r = m + 2$, so then $n_N = r$.

Let us now look at the multiplicities of zeros of $Q_N(j_N(z))$ defined by (7). Obviously, the set of zeros of $Q_N(j_N(z))$ coincides with the set of poles of $S(j_N)(z)/(j'_N(z))^2$. Moreover, if $e \in \mathcal{E}_N$ is a zero of j'_N of order $m_N(e)$, then we have the local expression

$$j_N(z) - j_N(e) = \frac{1}{(m_N(e) + 1)!}(z - e)^{m_N(e)+1} g_{N,e}(z),$$

where $g_{N,e}(z)$ is a holomorphic function such that $g_{N,e}(e) \neq 0$. Therefore, the point e is a zero of $Q_N(j_N(z))$ of order $2(m_N(e) + 1)$. This, together with Proposition 5 proves that the set of poles of $S(j_N)(z)/(j'_N(z))^2$ with corresponding orders coincides with the set of zeros of $Q_N(j_N(z))$ with corresponding orders. Consequently, we may take Q_r to be defined by (7).

It remains to prove that by taking $Q_N(y)$ to be given by (7), we then have that the lead coefficient of P_N is equal to one. From the q-expansion (4) and the fact that the q-expansion of $(j'_N(z))^4$ begins with $(2\pi)^4 q^{-4}$ we see that the q-expansion of $S(j_N)(z)/(j'_N(z))^2$ begins with $-\frac{1}{2}q^2$. Since the q-expansion of j_N is normalized so it begins with q^{-1} it is obvious that the q-expansion of $Q_N(j_N)$ begins with $2q^{-2} \cdot q^{-n_N}$, therefore, taking the lead coefficient of P_N to be equal to one we get that the q-expansion of the right hand side of (6) begins with $-\frac{1}{2}q^2$, which implies that P_N is monic.

Finally, the bound (8) for n_N follows from the above proved product expansion for Q_N, taking into account that P_N and Q_N may have common factors. □

4. Evaluating the coefficients of $R_N(y)$

4.1. **An algorithm.** There are three computational results to be obtained through computer assistance: The first evaluates the coefficients of both the numerator and the denominator of R_N; the second which determines the roots of the Q_N, the denominator of R_N, and the third approximates j_N at each elliptic point numerically, so then we can determine the specific values of $j_N(e)$.

The algorithm for computation of polynomials $P_N(x)$ and $Q_N(x)$ is the following.

Step 1. Fix N. Obtain from [9] the set $\mathcal{E}_N$ of elliptic points of X_N and, in an abuse of notation, define n_N by taking equality in (8).

Step 2. Use the exact expression of the Hauptmodul $j_N(z)$ in terms of Eisenstein series and the Kronecker limit function [16] to compute the q-expansion of $j_N(z)$, truncated at $O(q^{2n_N+2})$.

Step 3. Derive the q-expansions of $\dfrac{j_N'}{2\pi i}$, $\dfrac{j_N''}{(2\pi i)^2}$, $\dfrac{j_N'''}{(2\pi i)^3}$ and compute the q-expansions of $\dfrac{2S(j_N)(j_N')^2}{(2\pi)^4}$ and $\dfrac{(j_N')^4}{(2\pi)^4}$.

Step 4. Define

$$P_N(x) = x^{n_N} + \sum_{k=0}^{n_N-1} A_k x^k,$$

$$Q_N(x) = 2\big(x^{n_N+2} + \sum_{k=0}^{n_N+1} B_k x^k\big),$$

and solve

$$\frac{1}{2}Q_N(j_N)\frac{2S(j_N)(j_N')^2}{(2\pi)^4} + P_N(j)\frac{(j_N')^4}{(2\pi)^4} = 0 \tag{6a}$$

for the coefficients of P_N and Q_N by setting each coefficient in the q-expansion of (6a) equal to zero.

By Theorem 6 the coefficient of q^{-n_N-4} in the q-expansion of (6a) vanishes identically. Comparing coefficients of $q^{-n_N-3}, \dots, q^{n_N-2}$ in the q-expansion of (6a) results in $(2n_N+2)$ linear equations for the $(2n_N+2)$ unknowns $\{A_k\}_{k=0}^{n_N-1}$ and $\{B_k\}_{k=0}^{n_N+1}$. After implementing the algorithm, these equations turn out to be linearly independent for each N, hence there is a unique solution for the coefficients of P_N and Q_N.

For each square-free integer N such that the arithmetic group $\Gamma_0(N)^+$ has genus zero, we have evaluated the polynomials P_N and Q_N as described above. We observe that all coefficients are integers. Moreover, P_N and $\frac{1}{2}Q_N$ are monic polynomials with integer coefficients, and we conclude that their roots are *algebraic integers*.

Theorem 6, equation (7), connects the roots of the monic polynomials $\frac{1}{2}Q_N$ to the values of the Hauptmoduli j_N at the elliptic points of X_N. As a consequence, we have that each $j_N(e)$ is an *algebraic integer* at each elliptic point $e \in \mathcal{E}_N$ of the respective surface X_N.

4.2. **Hauptmodul values at elliptic points.** Having proven that the values of the Hauptmoduli at elliptic points are algebraic integers, we now compute these algebraic integers explicitly. As above, let us write $h_N(y) := \big(\frac{1}{2}Q_N(y)\big)^{1/2}$. According to (7), the function h_N is a monic polynomial and has the same roots as the polynomial Q_N. It remains to compute the roots.

To begin, we factor h_N into irreducible polynomials and use computer algebra to finally find explicit expressions for the roots in terms of radicals. From the expressions for Q_N, we obtain the following list for h_N, see Table 1.

Table 1: The list of monic polynomials h_N factored into irreducible polynomials.

$h_1(y) = (y+744)(y-984)$
$h_2(y) = (y+104)(y-152)$
$h_3(y) = (y+42)(y-66)$
$h_5(y) = (y+16)(y^2-12y-464)$
$h_6(y) = (y+14)(y+10)(y-22)$
$h_7(y) = (y+10)(y+9)(y-18)$
$h_{10}(y) = (y+8)(y+4)(y-12)$
$h_{11}(y) = (y+6)(y^3-2y^2-76y-212)$
$h_{13}(y) = (y+4)(y+3)(y^2-4y-48)$

$$
\begin{aligned}
h_{14}(y) &= (y+6)(y+2)(y^2-6y-23)\\
h_{15}(y) &= (y+4)(y-8)(y^2+6y+13)\\
h_{17}(y) &= (y+2)(y^4+2y^3-39y^2-176y-212)\\
h_{19}(y) &= (y+4)(y+3)(y^3-4y^2-16y-12)\\
h_{21}(y) &= (y+4)(y-0)(y^2-2y-27)\\
h_{22}(y) &= (y+2)(y-6)(y^3+6y^2+8y+4)\\
h_{23}(y) &= (y^3+6y^2+11y+7)(y^3-2y^2-17y-25)\\
h_{26}(y) &= (y+4)(y-0)(y^3-2y^2-15y-16)\\
h_{29}(y) &= (y+2)(y^6+2y^5-17y^4-66y^3-83y^2-32y-4)\\
h_{30}(y) &= (y+4)(y+3)(y-0)(y-1)(y-5)\\
h_{31}(y) &= (y-0)(y^3+4y^2+3y+1)(y^3-17y-27)\\
h_{33}(y) &= (y-0)(y^2-2y-11)(y^3+4y^2+8y+4)\\
h_{34}(y) &= (y+2)(y+1)(y^2+3y-2)(y^2-5y+2)\\
h_{35}(y) &= (y+2)(y^3-2y^2-4y-20)(y^2+2y+5)\\
h_{38}(y) &= (y-0)(y^3+4y^2+4y+4)(y^3-2y^2-7y-8)\\
h_{39}(y) &= (y+3)(y-1)(y^2+3y-1)(y^2-5y+3)\\
h_{41}(y) &= (y-0)(y^8+4y^7-8y^6-66y^5-120y^4-56y^3+53y^2+36y-16)\\
h_{42}(y) &= (y+3)(y-0)(y-1)(y-4)(y^2+3y+4)\\
h_{46}(y) &= (y^2-2y-7)(y^3+2y^2+y+1)(y^3+2y^2-3y+1)\\
h_{47}(y) &= (y^5+4y^4+7y^3+8y^2+4y+1)(y^5-5y^3-20y^2-24y-19)\\
h_{51}(y) &= (y+2)(y^3-2y^2-4y-4)(y^4+2y^3+3y^2-2y+1)\\
h_{55}(y) &= (y+1)(y^2+3y+1)(y^2-5y+5)(y^3+3y^2-y-7)\\
h_{59}(y) &= (y^3+2y^2+1)(y^9+2y^8-4y^7-21y^6-44y^5-60y^4-61y^3-46y^2-24y-11)\\
h_{62}(y) &= (y^3+4y^2+5y+3)(y^3+y-1)(y^4-2y^3-3y^2-4y+4)\\
h_{66}(y) &= (y+3)(y-0)(y-1)(y^2-y-8)(y^3-4y+4)\\
h_{69}(y) &= (y^3+4y^2+7y+5)(y^3-y+1)(y^4-2y^3-5y^2+6y-3)\\
h_{70}(y) &= (y+2)(y+1)(y-3)(y^2-y+2)(y^3+2y^2+4)\\
h_{71}(y) &= (y^7+4y^6+5y^5+y^4-3y^3-2y^2+1)(y^7-7y^5-11y^4+5y^3+18y^2+4y-11)\\
h_{78}(y) &= (y+1)(y-3)(y^2+y+1)(y^2+y-3)(y^3+y^2-4)\\
h_{87}(y) &= (y^3+2y^2+3y+3)(y^3-2y^2-y-1)(y^6+2y^5+7y^4+6y^3+13y^2+4y+8)\\
h_{94}(y) &= (y^4-2y^3-3y^2+4y-4)(y^5+4y^4+3y^3-2y^2+2y+5)(y^5-y^3+2y^2-2y+1)\\
h_{95}(y) &= (y-1)(y^3+y^2-y+3)(y^4+y^3-2y^2+2y-1)(y^4+y^3-6y^2-10y-5)\\
h_{105}(y) &= (y-1)(y^2+3y+3)(y^2-y-1)(y^2-y-5)(y^3+y^2-y-5)\\
h_{110}(y) &= (y-1)(y^2+y+3)(y^2+y-1)(y^3+y^2+3y-1)(y^3-y^2-8)\\
h_{119}(y) &= (y^4+2y^3+3y^2+6y+5)(y^5+2y^4+3y^3+6y^2+4y+1)(y^5-2y^4+3y^3-6y^2-7)
\end{aligned}
$$

For each level N, one then needs to identify different roots of $h_N(y)$ and match the roots with approximate values of the Hauptomuli $j_N(z)$. The list of roots of $h_N(y)$ and approximate values of the Hauptomuli $j_N(z)$ at elliptic points is given in appendices of the extended version [19] of this paper.

5. An application to explicit class field theory

Let $e \in \mathcal{E}_N$ be an order two element which is not a fixed point of some $\gamma \in \overline{\Gamma_0(N)}$. Then, in a slight abuse of notation, the point $e \in \mathbb{H}$ is a fixed point of the order two element

$$\gamma_e := \begin{pmatrix} a_e\sqrt{v} & b_e/\sqrt{v} \\ c_eN/\sqrt{v} & -a_e\sqrt{v} \end{pmatrix} \in \overline{\Gamma_0(N)^+} \setminus \overline{\Gamma_0(N)}, \quad \text{for some } v \mid N. \tag{9}$$

Equivalently, we see that $e \in \mathbb{H}$ is a zero of the quadratic polynomial

$$f_{\gamma_e}(X) := c_eNX^2 - 2a_evX - b_e \in \mathbb{Z}[X],$$

where we may assume that $c_e > 0$. The polynomial $f_{\gamma_e}(X)$ is irreducible in $\mathbb{Z}[X]$ with discriminant $-4v$ if $v \equiv 3 \mod 4$ and either b_e and c_e or b_e and N are both even. Otherwise, the polynomial $\frac{1}{2}f_{\gamma_e}(X)$ is irreducible in $\mathbb{Z}[X]$ with discriminant $-v$. Therefore, the complex lattice $\mathcal{L}_e$ generated by e and 1 is an invertible ideal for the quadratic order

$$\mathcal{O}_e = \begin{cases} \mathbb{Z}[\frac{v+\sqrt{-v}}{2}], & \text{for } v \equiv 3 \mod 4 \text{ and } b_e, c_e \text{ both even or } b_e, N \text{ both even;} \\ \mathbb{Z}[\sqrt{-v}], & \text{otherwise.} \end{cases}$$

With a slight abuse of notation, we will also say that $-4v$ and $-v$, respectively, are discriminants of the element e.

In the case when N is prime, from [8], Lemma 2.2 we have that the ideals $\mathcal{L}_e$ represent all ideal classes of $\mathcal{O}_e$. Therefore, in this case the class number of $\mathcal{O}_e$ is equal to the number of ideals $\mathcal{L}_e$. In other words, the class number of the order $\mathbb{Z}[\frac{N+\sqrt{-N}}{2}]$ is equal to the number of elements $e \in \mathcal{E}_N$ which are fixed points of order two elliptic elements γ_e given by (9) for which $N \equiv 3 \mod 4$ and b_e and c_e are both even. Analogously, the class number of the order $\mathbb{Z}[\sqrt{-N}]$ is equal to the number of elements $e \in \mathcal{E}_N$ which are fixed points of order two elliptic elements γ_e given by (9) for which the polynomial $f_{\gamma_e}(X)$ is an irreducible polynomial of discriminant $-4N$.

In the case when the level N is composite and, set $N_1 = N/v$ for any proper divisor $1 < v < N$ of N. Then we can write $f_{\gamma_e}(X) = (c_e N_1)vX^2 - 2a_e vX - b_e$. The number N_1 is odd, hence the numbers $c_e N_1$ and c_e are of the same parity. Every element of $\Gamma_0(N)^+$ of the form (9) belongs to $\Gamma_0(v)^+$, hence, for any divisor v of odd level N, the number of elements of $\mathcal{E}_N$ with discriminant equal $-4v$ or $-v$ is less than or equal to the number of elements of $\mathcal{E}_v$ with the same discriminant. In the case when the level N is even, for any divisor $2 < v < N$ the parity of $c_e N/v$ changes. The discriminant of the corresponding irreducible polynomial may change as well, so the above statement may not be true. For example, when $N = 10$ there is only one elliptic element $e = 1/2 + i\sqrt{5}/10 \in \mathcal{E}_5 \cap \mathcal{E}_{10}$ which has discriminant $-4 \cdot 5$, while there are two elements of $\mathcal{E}_5$ with the same discriminant. On the other hand, there are six elements of $\mathcal{E}_{46}$ with discriminant -23 while there are only three elements of $\mathcal{E}_{23}$ with the same discriminant.

Let $\widetilde{\mathcal{E}}_N$ denote the set of all elements of $\mathcal{E}_N$ which are order two and which are not fixed points of an order two elliptic element in $\Gamma_0(N)$. We have computed elliptic points in $\widetilde{\mathcal{E}}_N$ and their discriminants for all 43 square-free levels $N > 1$. It turned out that in all cases, except for the level $N = 46$ one has a bijection between the ideal classes of orders $\mathcal{O}_e$ and ideals $\mathcal{L}_e$ generated by e and 1, where $e \in \widetilde{\mathcal{E}}_N$ is a fixed point of the transformation (9) whose discriminant equals either $-4v$ or $-v$ when $v \mid N$ is prime. Moreover, the number of elliptic elements with discriminants equal to $-4v$ or $-v$ when v is composite number with l prime factors (which must be distinct, by our assumption on levels N) is equal to the class number of the corresponding order divided by 2^{l-1}. In case when $N = 46$ and $v = 23$, there are 6 elliptic points in $\mathcal{E}_{46}$ with discriminant -23. Later, we will see that we may group those points into two groups, each consisting of three points according to the factorization of $h_{46}(z)$ into irreducible factors. Tables 2 and 3 provide lists of the discriminants associated to elements of $\widetilde{\mathcal{E}}_N$.

Therefore, for all $N \neq 46$, we can write $\widetilde{\mathcal{E}}_N$ as the disjoint union

$$\widetilde{\mathcal{E}}_N = \biguplus_{v|N} \left(\widetilde{\mathcal{E}}_{N,-4v} \cup \widetilde{\mathcal{E}}_{N,-v} \right),$$

where $\widetilde{\mathcal{E}}_{N,-D}$ denotes the set of all elements of $\widetilde{\mathcal{E}}_N$ which are zeros of irreducible polynomials $f_{\gamma_e}(X)$ in $\mathbb{Z}[X]$ with discriminant $-D$. It is possible that some sets $\widetilde{\mathcal{E}}_{N,-D}$ are empty. Let $m_{N,-D}$ denote the number of elements of $\widetilde{\mathcal{E}}_{N,-D}$. From Tables 2 and 3, we deduce that, in the case when a divisor $v > 1$ of N is prime, the number $m_{N,-4v}$ is either zero or equals the class number of the order $\mathbb{Z}[\sqrt{-v}]$. Likewise, the non-zero number $m_{N,-v}$ is the class number of the order $\mathbb{Z}[\frac{v+\sqrt{-v}}{2}]$. When v is a product of l prime factors, the non-zero number $2^{l-1}m_{N,-4v}$ is equal to the class number of the order $\mathbb{Z}[\sqrt{-v}]$ while the non-zero number $2^{l-1}m_{N,-v}$ equals the class number of the order $\mathbb{Z}[\frac{v+\sqrt{-v}}{2}]$. (This follows from the fact that in the latter case, $\Gamma_0(v)^*$ is a subgroup of index 2^{l-1} in $\overline{\Gamma_0(v)^+}$.)

From an inspection of the values of $j_N(e)$ for $e \in \mathcal{E}_N$, $N \neq 46$ listed in [19], Appendix 3, one sees the following. For any element $e \in \widetilde{\mathcal{E}}_{N,-D} \neq \emptyset$, where $D = 4v$ or $D = v$ for some $v \mid N$, the value $j_N(e)$ is the zero of an irreducible polynomial $h_{N,D}(y) \in \mathbb{Z}[y]$ of degree $m_{N,-D}$ which is a factor of $h_N(y)$. In other words,

$$h_N(y) = \prod_{v|N} h_{N,4v}(y) h_{N,v}(y),$$

where, in the case when $\widetilde{\mathcal{E}}_{N,-D} = \emptyset$ for $D = 4v$ or $D = v$ we put $h_{N,D}(y) \equiv 1$. In the case when $N = 46$, the polynomial h_{46} is product of three irreducible, monic polynomials: two polynomials of degree 3, whose zeros are values of j_{46} at elliptic points with discriminant -23 and one degree two polynomial, whose zeros are values of j_{46} at elliptic points with discriminant $-4 \cdot 46$. With a slight ambiguity in the notation we will denote both such degree 3 polynomials by $h_{46,-23}$.

The results of [8] imply that $j_N(e)$ for all $e \in \widetilde{\mathcal{E}}_N$ belong to the ring class fields of the corresponding orders. Moreover, for prime divisors v of N, the non-trivial polynomials $h_{N,-4v}$ and $h_{N,-v}$ are irreducible polynomials of degree equal to the class number, hence they are generating polynomials of the ring class field of the corresponding order over $\mathbb{Q}[\sqrt{-v}]$. All non-trivial polynomials $h_{N,-4v}$ and $h_{N,-v}$ with prime v are listed in Table 2.

For composite divisors v of N with $l \geq 2$ prime factors, non-trivial polynomials $h_{N,-4v}$ and $h_{N,-v}$ are irreducible polynomials (over $\mathbb{Q}[\sqrt{-v}]$) of a degree equal to the class number of the corresponding order divided by 2^{l-1} and hence generate subfields of the corresponding class fields of index 2^{l-1}. The list of such polynomials is provided in Table 3.

The above discussion, together with results of [8], yields the following corollary of the Main Theorem.

Corollary 7. *Let N be a square-free number such that X_N has genus zero. With the above notation the following statements hold true:*

(i) *$j_N(e) \in \mathbb{Z}$ for all elliptic elements $e \in \mathcal{E}_N$ of order three or higher and for all order two elements of $\mathcal{E}_N$ which are fixed points of some order two elliptic elements from $\overline{\Gamma_0(N)}$.*

(ii) *Let $v \mid N$ be a prime such that $\widetilde{\mathcal{E}}_{N,-4v} \neq \emptyset$. Then the polynomial $h_{N,4v}(y)$ is the generating polynomial of the ring class field of the order $\mathbb{Z}[\sqrt{-v}]$ over $\mathbb{Q}[\sqrt{-v}]$.*

(iii) *Let $v \mid N$ be a prime such that $\widetilde{\mathcal{E}}_{N,-v} \neq \emptyset$. Then the polynomial $h_{N,v}(y)$ is the generating polynomial of the ring class field of the order $\mathbb{Z}[\frac{v+\sqrt{-v}}{2}]$ over $\mathbb{Q}[\sqrt{-v}]$.*

(iv) *Let $v \mid N$ be a composite number with l prime factors such that $\widetilde{\mathcal{E}}_{N,-4v} \neq \emptyset$. Then, the polynomial $h_{N,4v}(y)$ generates the subfield of the ring class field of the order $\mathbb{Z}[\sqrt{-v}]$ over $\mathbb{Q}[\sqrt{-v}]$ of index 2^{l-1} in the ring class field of $\mathbb{Z}[\sqrt{-v}]$.*

(v) *Let $v \mid N$ be a composite number with l prime factors such that $\widetilde{\mathcal{E}}_{N,-v} \neq \emptyset$. Then, the polynomial $h_{N,v}(y)$ generates the subfield of the ring class field of the order $\mathbb{Z}[\frac{v+\sqrt{-v}}{2}]$ over $\mathbb{Q}[\sqrt{-v}]$ of index 2^{l-1} in the ring class field of $\mathbb{Z}[\frac{v+\sqrt{-v}}{2}]$.*

Table 2: The table lists for all genus zero square-free levels $N > 1$ the discriminant D of the order two element from $\overline{\Gamma_0(N)^+} \setminus \overline{\Gamma_0(N)}$, provided $D = 4v$ and $D = v$, respectively, and v is a prime divisor of N. Listed is also the order generated by the elliptic element e such that f_{γ_e} and $\frac{1}{2}f_{\gamma_e}$, respectively, has discriminant D, the class number of the order, and the generating polynomial of the class field of the order over the corresponding imaginary quadratic extension of $\mathbb{Q}$.

N	D	Order	Class number	Generating polynomial
2	$-4\cdot 2$	$\mathbb{Z}[\sqrt{-2}]$	1	$y-152$
3	$-4\cdot 3$	$\mathbb{Z}[\sqrt{-3}]$	1	$y-66$
5	$-4\cdot 5$	$\mathbb{Z}[\sqrt{-5}]$	2	$y^2-12y-464$
7	$-4\cdot 7$	$\mathbb{Z}[\sqrt{-7}]$	1	$y-18$
7	-7	$\mathbb{Z}[7/2+\sqrt{-7}/2]$	1	$y+10$
11	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	$y^3-2y^2-76y-212$
11	-11	$\mathbb{Z}[11/2+\sqrt{-11}/2]$	1	$y+6$
13	$-4\cdot 13$	$\mathbb{Z}[\sqrt{-13}]$	2	$y^2-4y-48$
15	$-4\cdot 5$	$\mathbb{Z}[\sqrt{-5}]$	2	$y^2+6y+13$
17	$-4\cdot 17$	$\mathbb{Z}[\sqrt{-17}]$	4	$y^4+2y^3-39y^2-176y-212$
19	$-4\cdot 19$	$\mathbb{Z}[\sqrt{-19}]$	3	$y^3-4y^2-16y-12$
19	-19	$\mathbb{Z}[19/2+\sqrt{-19}/2]$	1	$y+4$
21	$-4\cdot 3$	$\mathbb{Z}[\sqrt{-3}]$	1	$y+4$
22	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	y^3+6y^2+8y+4
23	$-4\cdot 23$	$\mathbb{Z}[\sqrt{-23}]$	3	$y^3-2y^2-17y-25$
23	-23	$\mathbb{Z}[23/2+\sqrt{-23}/2]$	3	$y^3+6y^2+11y+7$
29	$-4\cdot 29$	$\mathbb{Z}[\sqrt{-29}]$	6	$y^6+2y^5-17y^4-66y^3-83y^2-32y-4$
31	$-4\cdot 31$	$\mathbb{Z}[\sqrt{-31}]$	3	$y^3-17y-27$
31	-31	$\mathbb{Z}[31/2+\sqrt{-31}/2]$	3	y^3+4y^2+3y+1
33	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	y^3+4y^2+8y+4
33	-11	$\mathbb{Z}[11/2+\sqrt{-11}/2]$	1	y
35	$-4\cdot 5$	$\mathbb{Z}[\sqrt{-5}]$	2	y^2+2y+5
39	$-4\cdot 3$	$\mathbb{Z}[\sqrt{-3}]$	1	$y-1$
41	$-4\cdot 41$	$\mathbb{Z}[\sqrt{-41}]$	8	$y^8+4y^7-8y^6-66y^5-120y^4-56y^3+53y^2+36y-16$
46	-23	$\mathbb{Z}[23/2+\sqrt{-23}/2]$	3	y^3+2y^2+y+1
46	-23	$\mathbb{Z}[23/2+\sqrt{-23}/2]$	3	y^3+2y^2-3y+1
47	$-4\cdot 47$	$\mathbb{Z}[\sqrt{-47}]$	5	$y^5-5y^3-20y^2-24y-19$
47	-47	$\mathbb{Z}[47/2+\sqrt{-47}/2]$	5	$y^5+4y^4+7y^3+8y^2+4y+1$
51	$-4\cdot 17$	$\mathbb{Z}[\sqrt{-17}]$	4	$y^4+2y^3+3y^2-2y+1$
55	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	y^3+3y^2-y-7

55	-11	$\mathbb{Z}[11/2+\sqrt{-11}/2]$	1	$y+1$
59	$-4\cdot 59$	$\mathbb{Z}[\sqrt{-59}]$	9	$y^9+2y^8-4y^7-21y^6-44y^5-60y^4-61y^3-46y^2-24y-11$
59	-59	$\mathbb{Z}[59/2+\sqrt{-59}/2]$	3	y^3+2y^2+1
62	$-4\cdot 31$	$\mathbb{Z}[\sqrt{-31}]$	3	y^3+4y^2+5y+3
62	-31	$\mathbb{Z}[31/2+\sqrt{-31}/2]$	3	y^3+y-1
66	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	y^3-4y+4
69	$-4\cdot 23$	$\mathbb{Z}[\sqrt{-23}]$	3	y^3+4y^2+7y+5
69	-23	$\mathbb{Z}[23/2+\sqrt{-23}/2]$	3	y^3-y+1
71	$-4\cdot 71$	$\mathbb{Z}[\sqrt{-71}]$	7	$y^7-7y^5-11y^4+5y^3+18y^2+4y-11$
71	-71	$\mathbb{Z}[71/2+\sqrt{-71}/2]$	7	$y^7+4y^6+5y^5+y^4-3y^3-2y^2+1$
87	$-4\cdot 29$	$\mathbb{Z}[\sqrt{-29}]$	6	$y^6+2y^5+7y^4+6y^3+13y^2+4y+8$
94	$-4\cdot 47$	$\mathbb{Z}[\sqrt{-47}]$	5	$y^5+4y^4+3y^3-2y^2+2y+5$
94	-47	$\mathbb{Z}[47/2+\sqrt{-47}/2]$	5	$y^5-y^3+2y^2-2y+1$
95	$-4\cdot 19$	$\mathbb{Z}[\sqrt{-19}]$	3	y^3+y^2-y+3
95	-19	$\mathbb{Z}[19/2+\sqrt{-19}/2]$	1	$y-1$
105	$-4\cdot 5$	$\mathbb{Z}[\sqrt{-5}]$	2	y^2-y-1
110	$-4\cdot 11$	$\mathbb{Z}[\sqrt{-11}]$	3	y^3+y^2+3y-1
119	$-4\cdot 17$	$\mathbb{Z}[\sqrt{-17}]$	4	$y^4+2y^3+3y^2+6y+5$

Table 3: The table lists for all genus zero square-free levels $N>1$ the discriminant D of the order two element from $\overline{\Gamma_0(N)^+}\setminus\overline{\Gamma_0(N)}$, provided $D=4v$ and $D=v$, respectively, and v is a composite divisor of N. Also listed is the order generated by the elliptic element e such that f_{γ_e} and $\frac{1}{2}f_{\gamma_e}$, respectively, has discriminant D, the class number of the order, the index of the subfield in the class field, and the generating polynomial of the subfield of the class field of the order over the corresponding imaginary quadratic extension of $\mathbb{Q}$.

N	D	Order	Class Number	Index	Generating polynomial
6	$-4\cdot 6$	$\mathbb{Z}[\sqrt{-6}]$	2	2	$y-22$
10	$-4\cdot 10$	$\mathbb{Z}[\sqrt{-10}]$	2	2	$y-12$
14	$-4\cdot 14$	$\mathbb{Z}[\sqrt{-14}]$	4	2	$y^2-6y-23$
15	$-4\cdot 15$	$\mathbb{Z}[\sqrt{-15}]$	2	2	$y-8$
15	-15	$\mathbb{Z}[15/2+\sqrt{-15}/2]$	2	2	$y+4$
21	$-4\cdot 21$	$\mathbb{Z}[\sqrt{-21}]$	4	2	$y^2-2y-27$
22	$-4\cdot 22$	$\mathbb{Z}[\sqrt{-22}]$	2	2	$y-6$
26	$-4\cdot 26$	$\mathbb{Z}[\sqrt{-26}]$	6	2	$y^3-2y^2-15y-16$
30	$-4\cdot 30$	$\mathbb{Z}[\sqrt{-30}]$	4	4	$y-5$
33	$-4\cdot 33$	$\mathbb{Z}[\sqrt{-33}]$	4	2	$y^2-2y-11$
34	$-4\cdot 34$	$\mathbb{Z}[\sqrt{-34}]$	4	2	y^2-5y+2
35	$-4\cdot 35$	$\mathbb{Z}[\sqrt{-35}]$	6	2	$y^3-2y^2-4y-20$
35	-35	$\mathbb{Z}[35/2+\sqrt{-35}/2]$	2	2	$y+2$
38	$-4\cdot 38$	$\mathbb{Z}[\sqrt{-38}]$	6	2	y^3-2y^2-7y-8
39	$-4\cdot 39$	$\mathbb{Z}[\sqrt{-39}]$	4	2	y^2-5y+3
39	-39	$\mathbb{Z}[39/2+\sqrt{-39}/2]$	4	2	y^2+3y-1
42	$-4\cdot 42$	$\mathbb{Z}[\sqrt{-42}]$	4	4	$y-4$
42	$-4\cdot 14$	$\mathbb{Z}[\sqrt{-14}]$	4	2	y^2+3y+4
46	$-4\cdot 46$	$\mathbb{Z}[\sqrt{-46}]$	4	2	y^2-2y-7
51	$-4\cdot 51$	$\mathbb{Z}[\sqrt{-51}]$	6	2	y^3-2y^2-4y-4
51	-51	$\mathbb{Z}[51/2+\sqrt{-51}/2]$	2	2	$y+2$
55	$-4\cdot 55$	$\mathbb{Z}[\sqrt{-55}]$	4	2	y^2-5y+5
55	-55	$\mathbb{Z}[55/2+\sqrt{-55}/2]$	4	2	y^2+3y+1
62	$-4\cdot 62$	$\mathbb{Z}[\sqrt{-62}]$	8	2	$y^4-2y^3-3y^2-4y+4$
66	$-4\cdot 66$	$\mathbb{Z}[\sqrt{-66}]$	8	4	y^2-y-8
69	$-4\cdot 69$	$\mathbb{Z}[\sqrt{-69}]$	8	2	$y^4-2y^3-5y^2+6y-3$
70	$-4\cdot 70$	$\mathbb{Z}[\sqrt{-70}]$	4	4	$y-3$
70	$-4\cdot 14$	$\mathbb{Z}[\sqrt{-14}]$	4	2	y^2-y+2

70	$-4\cdot 35$	$\mathbb{Z}[\sqrt{-35}]$	6	2	y^3+2y^2+4
78	$-4\cdot 78$	$\mathbb{Z}[\sqrt{-78}]$	4	4	$y-3$
78	$-4\cdot 26$	$\mathbb{Z}[\sqrt{-26}]$	6	2	y^3+y^2-4
78	$-4\cdot 39$	$\mathbb{Z}[\sqrt{-39}]$	4	2	y^2+y-3
78	-39	$\mathbb{Z}[39/2+\sqrt{-39}/2]$	4	2	y^2+y+1
87	$-4\cdot 87$	$\mathbb{Z}[\sqrt{-87}]$	6	2	y^3-2y^2-y-1
87	-87	$\mathbb{Z}[87/2+\sqrt{-87}/2]$	6	2	y^3+2y^2+3y+3
94	$-4\cdot 94$	$\mathbb{Z}[\sqrt{-94}]$	8	2	$y^4-2y^3-3y^2+4y-4$
95	$-4\cdot 95$	$\mathbb{Z}[\sqrt{-95}]$	8	2	$y^4+y^3-6y^2-10y-5$
95	-95	$\mathbb{Z}[95/2+\sqrt{-95}/2]$	8	2	$y^4+y^3-2y^2+2y-1$
105	$-4\cdot 105$	$\mathbb{Z}[\sqrt{-105}]$	8	4	y^2-y-5
105	$-4\cdot 35$	$\mathbb{Z}[\sqrt{-35}]$	6	2	y^3+y^2-y-5
105	-35	$\mathbb{Z}[35/2+\sqrt{-35}/2]$	2	2	$y+1$
105	$-4\cdot 21$	$\mathbb{Z}[\sqrt{-21}]$	4	2	y^2+3y+3
110	$-4\cdot 110$	$\mathbb{Z}[\sqrt{-110}]$	12	4	y^3-y^2-8
110	$-4\cdot 55$	$\mathbb{Z}[\sqrt{-55}]$	4	2	y^2+y-1
110	-55	$\mathbb{Z}[55/2+\sqrt{-55}/2]$	4	2	y^2+y+3
119	$-4\cdot 119$	$\mathbb{Z}[\sqrt{-119}]$	10	2	$y^5-2y^4+3y^3-6y^2-7$
119	-119	$\mathbb{Z}[119/2+\sqrt{-119}/2]$	10	2	$y^5+2y^4+3y^3+6y^2+4y+1$

In certain cases, when the class number of the class field is not a power of 2, we are able to deduce class fields of the corresponding orders, by looking at the genus fields of the imaginary quadratic fields and checking that the generating polynomials of the subfields of the ring class field are irreducible over genus fields (for a definition, see [7], p. 121). In cases when the class number is a power of 2, the generating polynomials appearing in Table 3 above are all reducible over genus fields; actually they are generating polynomials for genus fields.

For example, when $N=26$, according to [7], Theorem 6.1. the genus field of $K=\mathbb{Q}[\sqrt{-26}]$ is $K[\sqrt{13}]$. A simple computation using Mathematica shows that both $y^3-2y^2-15y-16$ and y^3+y^2-4 are irreducible over $K[\sqrt{13}]$. Denoting by α the real zero of e.g. y^3+y^2-4, we see that $K[\sqrt{13},\alpha]$ is a degree 6 extension of K and the subfield of the ring class field L of the order $\mathbb{Z}[\sqrt{-26}]$ over K, hence $L=K[\sqrt{13},\alpha]$. Arguing in the same way, we deduce the following: The ring class field of $\mathbb{Z}[\sqrt{-35}]$ over $K=\mathbb{Q}[\sqrt{-35}]$ is $K[\sqrt{5},\alpha]$ where α is a real zero of $y^3-2y^2-4y-20$ or y^3+2y^2+4 or y^3+y^2-y-5; The ring class field of $\mathbb{Z}[\sqrt{-38}]$ over $K=\mathbb{Q}[\sqrt{-38}]$ is $K[\sqrt{2},\alpha]$ where α is a real zero of y^3-2y^2-7y-8; The ring class field of $\mathbb{Z}[\sqrt{-51}]$ over $K=\mathbb{Q}[\sqrt{-51}]$ is $K[\sqrt{-3},\alpha]$ where α is a real zero of y^3-2y^2-4y-4; The ring class field of $\mathbb{Z}[\sqrt{-87}]$ over $K=\mathbb{Q}[\sqrt{-87}]$ is $K[\sqrt{-3},\alpha]$ where α is a real zero of y^3-2y^2-y-1; The ring class field of $\mathbb{Z}[87/2+\sqrt{-87}/2]$ over $K=\mathbb{Q}[\sqrt{-87}]$ is $K[\sqrt{-3},\alpha]$ where α is a real zero of y^3+2y^2+3y+3; The ring class field of $\mathbb{Z}[\sqrt{-110}]$ over $K=\mathbb{Q}[\sqrt{-110}]$ is $K[\sqrt{2},\sqrt{5},\alpha]$ where α is a real zero of y^3-y^2-8; The ring class field of $\mathbb{Z}[\sqrt{-119}]$ over $K=\mathbb{Q}[\sqrt{-119}]$ is $K[\sqrt{-7},\alpha]$ where α is a real zero of $y^5-2y^4+3y^3-6y^2-7$; The ring class field of $\mathbb{Z}[119/2+\sqrt{-119}/2]$ over $K=\mathbb{Q}[\sqrt{-119}]$ is $K[\sqrt{-7},\alpha]$ where α is a real zero of $y^5+2y^4+3y^3+6y^2+4y+1$.

References

[1] A. O. L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[2] R. E. Borcherds, Monstrous moonshine and monstrous Lie superalgebras, Invent. Math. **109** (1992), 405–444.

[3] *Seminar on complex multiplication*, eds. A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, J. P. Serre, Lecture Notes in Mathematics **21** Springer-Verlag, Berlin-New York, 1966.

[4] I. Chen, N. Yui, Singular values of Thompson series. In *Groups, difference sets, and the Monster* (Columbus, OH, 1993), 255–326, Ohio State University Mathematics Research Institute Publications, 4, de Gruyter, Berlin, 1996.

[5] S. Y. Choi, J. K. Koo, Class fields from the fundamental Thompson series of level $N=o(g)$, J. Korean. Math. Soc. **42** No. 2 (2005), 203–222.

[6] J. H. Conway, S. P. Norton, Monstrous moonshine, Bull. London Math. Soc. **11** (1979), 308–339.

[7] D. Cox, Primes of the form x^2+ny^2, John WileySons, New York.

[8] D. Cox, J. McKay, P. Stevenhagen, Principal moduli and class fields, Bull. London Math. Soc. **36** vol. 1 (2004), 3–12.

[9] C. J. Cummins, Congruence subgroups of groups commensurable with $\mathrm{PSL}(2,\mathbb{Z})$ of genus 0 and 1, Experiment. Math. **13** (2004), 361–382.

[10] J. Freitag and T. Scanlon, Strong minimality and the j-function, `http://arxiv.org/abs/1402.4588`

[11] B. Gross, D. Zagier, On singular moduli, J. Reine Angew. Math. **355** (1985), 191–220.

[12] J. Harnad, J. McKay, Modular solutions to equations of generalized Halphen type, Proc. R. Soc. Lond. A **456** (2000), 261–294.

[13] T. Granlund, *GMP – The GNU Multiple Precision Arithmetic Library, Version 5.0.5*; 2012, `https://gmplib.org/`

[14] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.9*; 2015, `http://www.gap-system.org`

[15] J. Jorgenson, L. Smajlović, and H. Then, On the distribution of eigenvalues of Maass forms on certain moonshine groups, Math. Comp. **83** (2014), 3039–3070.
[16] J. Jorgenson, L. Smajlović, and H. Then, Kronecker's limit formula, holomorphic modular functions and q-expansions on certain arithmetic groups, Experiment. Math. **25** No. 3 (2016), 295-320.
[17] J. Jorgenson, L. Smajlović, and H. Then, Certain aspects of holomorphic function theory on some genus zero arithmetic groups, LMS J. Comput. Math. **19** (2016), no. 2, 360–381.
[18] J. Jorgenson, L. Smajlović, and H. Then, data page `http://www.efsa.unsa.ba/~lejla.smajlovic/`
[19] J. Jorgenson, L. Smajlović, and H. Then, The Hauptmodul at elliptic points of certain arithmetic groups, arXiv:1602.07426.
[20] D. Masser, Heights, transcendence, and linear independence on commutative group varieties. In *Diophantine approximation (Cetraro 2000)*, Lecture Notes in Mathematics **1819**, Springer, Berlin, 2003, 1–51.
[21] The PARI Group, *PARI/GP version 2.5.1*, Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`.
[22] T. Schneider, Arithmetische Untersuchungen elliptischer Integrale, Math. Annalen **113** (1937), 1–13,
[23] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, **7**, Springer-Verlag, New York, 1973.
[24] C. L. Siegel, *Transcendental Numbers*, Annals of Mathematics Studies, **16**, Princeton University Press, Princeton, NJ, 1949.
[25] D. Zagier, Traces of singular moduli. In *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, 211–244.

Department of Mathematics, The City College of New York, Convent Avenue at 138th Street, New York, NY 10031 USA, e-mail: jjorgenson@mindspring.com

Department of Mathematics, University of Sarajevo, Zmaja od Bosne 35, 71 000 Sarajevo, Bosnia and Herzegovina, e-mail: lejlas@pmf.unsa.ba

Alemannenweg 1, 89537 Giengen, Germany, e-mail: holger.then@bristol.ac.uk